МОДЕЛЬ РОЗПОДІЛЕНИХ АТАК У МЕРЕЖАХ ЗВ'ЯЗКУ 5G

Коляденко Ю.Ю., Бадеєв В.О.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна.

E-mail: yuliia.koliadenko@nure.ua,
valerii.badieiev@nure.ua

Abstract

It is shown that the 5G network architecture is not without potential vulnerabilities from an information security point of view. The controller, as a key component in managing the entire network infrastructure, is the most vulnerable element, an attack on which can lead to critical consequences for the entire infrastructure. The main threats arising from network devices remain variations of attacks such as denial of service, controller spoofing, etc. A mathematical model of the 5G network in the form of a queuing system has been developed. The advantages of the proposed model are the possibility of timely (early) attack detection and its ability to adapt to real network parameters.

Вступ

Мережа стільникового зв'язку характеризується величезною вартістю та великими термінами будівництва. Зміни у стандартах зв'язку відбуваються регулярно, але перехід до нового стандарту потребує нових вкладень та заміни обладнання, яке часто ще не виробило свій ресурс. Зараз для запуску мережі 5G все стає простіше завдяки технології програмних мереж, що конфігуруються. У мережах 5G основні функції комутаторів та маршрутизаторів перенесені на центральний мережевий контролер, що спрощує застосування мережевих політик, та моніторинг стану мережі. При такому підході передавальні пристрої відповідають лише за передачу даних, спираючись на таблицю потоків, яка будується централізованим мережевим контролером, що взаємодіє з передавальним пристроєм [1].

Взаємодія між мережним контролером і передавальними пристроями реалізується за допомогою програмного інтерфейсу, який використовується для прямого управління групами пристроїв [1,2]. Архітектура комутатора базується на одній чи декількох таблицях правил, які визначають механізм обробки потоків мережного трафіку. Кожне правило є записом у таблиці комутатора. Запис зіставляється з певним потоком трафіку. Залежно від результату зіставлення, застосовується відповідна дія (блокування, передача, модифікація тощо) до пакетів з даного потоку.

Архітектура мережі, припускаючи істотно інший підхід до реалізації мережевої інфраструктури, не позбавлена потенційних вразливостей з погляду інформаційної безпеки. Необхідність поділу доступу мережевих додатків при роботі з контролером, питання аутентифікації та авторизації при роботі додатків з контролером – це лише мала частина аспектів безпеки, які доводиться брати до уваги при проектуванні мереж [1]. Контролер як ключовий компонент в управлінні усією інфраструктурою мережі є найуразливішим елементом, атака на який може спричинити критичні для всієї інфраструктури наслідки [3]. Таким чином, розробка моделі розподілених атак у мережах 5G є актуальним науковим завданням.

1. Основні загрози архітектури 5G

Основними загрозами, що виникають з боку мережевих пристроїв, залишаються варіації таких атак, як "відмова в обслуговуванні", заміна контролера і т.д. Перенесення «аналітичної» компоненти мережі на контролер природним чином переносить акцент багатьох атак з мережевого обладнання на програмне забезпечення, що забезпечує функціонування мережі: контролер мережі та мережеві додатки, що звертаються до контролера [4].

Найбільш простим і одночасно ефективним способом порушення цілісності роботи мережі 5G є атаки типу "відмова в обслуговуванні". Небезпека атаки випливає із самого алгоритму роботи комутатора при отриманні невідомого пакета. У такій ситуації можливі два варіанти:

1. Пакет повністю вирушає на контролер для аналізу.

2. Пакет залишається у пам'яті комутатора, на контролер відправляються виключно заголовки пакета.

Обидва способи залишають для атакуючого широке поле ефективної реалізації відмови в обслуговуванні шляхом формування потоку різних пакетів в мережі. Розглянемо реакцію мережі в обох вищенаведених випадках [1]:

1. Комутатор починає формування великої кількості повідомлень передачі невідомих пакетів на контролер. Витрачаються процесорні ресурси комутатора, збільшується витрата пам'яті. Особливо сильно витрачається пам'ять у разі, якщо комутатор буферизує самі пакети і пересилає контролеру лише заголовки.

2. Потік пакетів від комутатора на контролер навантажує канал зв'язку між контролером та комутатором. Якщо середовище зв'язку поділяється, то зниження оперативності доставки повідомлень можуть відчути на собі всі комутатори. Підвищений вплив на канал зв'язку буде в ситуації, коли комутатор пересилає пакети для аналізу повністю.

3. Контролер приймає та обробляє потік повідомлень, витрачаючи процесорний час та пам'ять свого середовища виконання. Формування черг повідомлень змусить легітимні повідомлення чекати на свою чергу і знизить оперативність прийняття рішень у мережі.

4. Контролер генерує потік різних повідомлень у відповідь на запити атакованного комутатора. Витрачаються ресурси каналу зв'язку між комутатором та контролерами.

5. Комутатор приймає команди від контролера та виконує їх, витрачаючи ресурси процесора та пам'ять. Якщо команди містять у собі створення нових правил таблиць потоків, відбувається їх лавиноподібне збільшення, час перевірки кожного нового пакета за таблицею збільшується, зростають витрати на обслуговування такої таблиці, а також можливе переповнення таблиць потоків.

В результаті реалізація атаки може призвести до наступних наслідків [1]:

1. Вичерпання ресурсів комутатора. Легітимні пакети або взагалі не будуть оброблені даним мережним вузлом, або їх обробка супроводжуватиметься затримками.

2. Канал зв'язку між контролером і комутатором не забезпечить доставки повідомлень управління, якщо він є завантаженим потоками даних.

3. Контролер буде перевантажений запитами, що надходять, і не зможе обробляти керуючі повідомлення, викликані легітимним трафіком.

Загрози безпеки, актуальні для більшості інформаційних систем, такі як сканування портів та визначення мережевих служб, є критичними для архітектури мережі через вразливість каналу та наявність великої кількості трафіку управління, що передається між комутаторами та мережевими контролерами. Відзначимо, що вразливість архітектури мережі до DoS/DDoS-атак є одним із найнебезпечніших для архітектури з централізованим управлінням.

Однією з причин вразливості мереж до атак заміни є надмірна гнучкість стандарту 5G. Стандарт дозволяє реалізувати взаємодію між мережним контролером та комутаторами на базі протоколу TCP без шифрування, а підтримка протоколу TLS є необов'язковою для реалізації.

Реакцію мережі на потоки різних пакетів, у тому числі і на атаки, можна розглядати як функціонування деякої системи масового обслуговування (СМО), яка обробляє вимоги на обробку пакетів.

2. Математична модель системи масового обслуговування

Під СМО [5] зазвичай розуміється сукупність обслуговуючих приладів і вимог (заявок) з деякого вхідного потоку вимог.

Число приладів у СМО може бути будь-яким. Основною характеристикою пристрою є час обслуговування однієї вимоги цим приладом. Цей показник характеризує не якість обслуговування, а пропускну здатність приладу. Час обслуговування зазвичай є непостійним. Він залежить від різних факторів. Тому у загальному випадку ця величина є випадковою [6]. При цьому вважається, що тривалість обслуговування різних вимог одним приладом є незалежні випадкові величини з тим самим законом розподілу. Найчастіше припускають, що цей закон є показовим. Його застосовують у тих випадках, коли час обслуговування переважної більшості вимог замало і лише для порівняно невеликої частини вимог воно велике. При показовому розподілі часу обслуговування вимог теоретичні міркування знач-

но спрощуються, і багато остаточних результатів виявляються справедливими і для довільного закону розподілу, але з тим самим середнім часом обслуговування.

Так само в теорії масового обслуговування прийнято вважати, що вхідний потік вимог розподілено за пуасонівським законом розподілу. За визначенням пуасонівський потік повинен задовольняти трьом наступним вимогам: стаціонарності, відсутності наслідків та ординарності.

Потік називається стаціонарним, якщо ймовірність надходження вимог протягом проміжку часу не залежить від початку цього проміжку.

Під відсутністю наслідку розуміється те, що ймовірність надходжень вимог до системи після довільного моменту часу не залежить від того, коли і скільки надійшло вимог до цього моменту. З цього випливає взаємна незалежність надходження тієї чи іншої кількості вимог на обслуговування в проміжки часу, що не перетинаються.

Властивість ординарності означає практичну неможливість одночасного надходження двох або більше вимог.

Варто зазначити, що багато реальних потоків є приблизно пуассонівськими. Пуасонівський потік повністю визначається одним параметром – інтенсивністю потоку.

Математичний апарат теорії масового обслуговування дозволяє визначити основні параметри системи: середня кількість зайнятих приладів, вірогідність відмови в обслуговуванні вимоги, середню довжину черги, середній час простою вимоги в черзі і т.д.

У цьому випадку найбільший інтерес становить середня кількість зайнятих приладів [6]:

В даному випадку найбільшу цікавість представляє середнє число зайнятих приладів [6]:

$$N = \sum_{k=1}^{n} k \cdot p_k = p_0 \sum_{k=1}^{n} \frac{\alpha^k}{(k-1)!} = \alpha(1 - p_n), \tag{1}$$

где n – кількість приладів у системі,, $\alpha = \lambda / \mu$, λ - інтенсивність потоку вимог, $1/\mu$ - математичне очікування часу обслуговування однієї вимоги. p_k - ймовірність знаходження в системі рівно k вимог:

$$p_k = \frac{a^n}{k! \sum_{i=0}^{n} \frac{a^i}{i!}}. \tag{2}$$

3. Потік вимог СМО

Розглянемо множину пакетів або їх заголовків, що надходять від комутатора до контролера, в якості вхідного потоку заявок. Покажемо, що за певних умов цей потік можна вважати пуассонівським.

Інтенсивність цього потоку може залежати від часу, якщо розглядати його протягом достатньо великих проміжків часу. Наприклад, протягом доби вдень його інтенсивність може бути більшою, ніж уночі. Тим не менш, при зменшенні тривалості аналізованого проміжку інтенсивність заявок, що надходять, стабілізується і може розглядатися як деяка постійна величина. Для різних мереж тривалість такого проміжку може бути різною (як правило, від кількох хвилин до кількох годин) і може бути встановлена експериментально.

В цьому випадку ймовірність надходження k вимог в інтервалі часу $(0,t)$ дорівнює ймовірності надходження k вимог у будь-якому іншому інтервалі тієї ж тривалості $(a,a+t)$ в межах заданого проміжку. Таким чином, потік, що розглядається, має властивість стаціонарності.

Далі вважатимемо, що комутатори звертаються до ресурсів контролера незалежно один від одного. Якщо при одному зверненні комутатора до контролера встановлюється одне з'єднання, то потік вимог має властивість відсутності післядії [5].

Покажемо, що потік вимог є ординарним. Розглянемо контролер із одним мережним інтерфейсом. За таким підключенням одночасно не можуть прийти одразу декілька пакетів.

Відповідно, існує деякий малий проміжок часу, протягом якого може надійти не більше однієї заявки. Отже, для контролера з одним інтерфейсом мережі вхідний потік пакетів є ординарним.

Таким чином, потік заявок, що містять пакети, що надходять на сервер з одним мережним інтерфейсом, має властивості стаціонарності, ординарності та відсутності післядії, і відповідно до визначення такий потік є пуассонівським.

4. 5G мережа у вигляді системи масового обслуговування

Оскільки потік вхідних на контролер пакетів у заданих умовах є пуассонівським, то його можна розглядати як потік вимог, які потрапляють до СМО. У нормальному режимі роботи у відповідь на кожен отриманий пакет контролер повинен відправити згенероване повідомлення на комутатор [5]. З того, що існує взаємноодназначна відповідність між вхідними та вихідними пакетами, випливає еквівалентність потоків. Далі в якості вимог СМО будемо розглядати пакети, що відправляються комутатором. Множиною обслуговуючих приладів будемо вважати ресурси комутатора і контролера, які призначені для зберігання параметрів TCP з'єднань. У такій інтерпретації обслуговування вимоги – це резервування відповідних ресурсів або до успішного встановлення TCP з'єднання, або до закінчення відведеного таймауту.

Для такої моделі ознакою атаки є різке збільшення кількості заявок до СМО. Перебуваючи під впливом атаки, комутатор та контролер виділяють відповідні ресурси, які залишаються зайнятими протягом відведеного таймауту. Часу таймауту (від десятків секунд до декількох хвилин) достатньо, щоб зайняти всі доступні ресурси комутатора та контролера, призначені для зберігання параметрів TCP з'єднань. Для моделі, що розглядається це означає різке збільшення зайнятих обслуговуючих приладів.

Розглянемо детальніше ресурси комутатора і контролера, які виступають в якості обслуговуючих приладів. Параметри TCP з'єднань зберігаються у відповідному буфері, який можна представити у вигляді масиву розмірності L, елементи якого зберігають параметри TCP з'єднань. Їх можна розділити на три типи: які містять параметри встановлених з'єднань, напіввідкритих з'єднань та вільні. Нехай B – кількість відкритих TCP з'єднань. Тоді $n = L - B$ – кількість елементів другого та третього типів, сукупність яких розглядатимемо як множину обслуговуючих приладів СМО. При цьому зайняті обслуговуванням вимог прилади – це елементи другого типу.

Залежно від співвідношення інтенсивності вхідного потоку вимог та розмірності масиву можна розглядати два типи СМО. Якщо інтенсивність вхідного потоку заявок значно менша за можливості контролера, то доцільно розглядати СМО з нескінченним числом обслуговуючих приладів. В іншому випадку можна розглядати СМО з відмовами. Зважаючи на те, що на практиці в нормальному режимі роботи можливості контролера зі значним запасом покривають вхідні вимоги, то розгляд системи з відмовами є неактуальним. Надалі будемо розглядати систему першого типу.

5. СМО з нескінченною кількістю обслуговуючих приладів

Позначимо відношення інтенсивності вхідного потоку вимог λ до середнього часу обслуговування заявки μ коефіцієнтом $\alpha = \lambda / \mu$. Так як потік вимог є пуасонівським, то ймовірність того, що в системі знаходиться рівно k вимог, визначається як:

$$p_k = \frac{\alpha^k e^{-\alpha}}{k!}. \tag{3}$$

Підставивши це значення у співвідношення (2), що описує середню кількість приладів, зайнятих обслуговуванням (загальна кількість напіввідкритих з'єднань) отримаємо:

$$N = \sum_{k=1}^{\infty} k \cdot p_k = p_0 \sum_{k=1}^{\infty} \frac{\alpha^k}{(k-1)!} = \alpha(1 - p_\infty). \tag{4}$$

Відповідно,

$$p_\infty = \lim_{k \to \infty} \frac{\alpha^k e^{-\alpha}}{k!} = e^{-\alpha} \lim_{k \to \infty} \frac{\alpha^k}{k!} = 0. \tag{5}$$

Зі співвідношень (4) і (5) для СМО з нескінченним числом обслуговуючих приладів маємо [6]:

$$N = \alpha(1 - p_\infty) = \alpha(1 - 0) = \alpha. \tag{6}$$

Запропонована модель описує роботу контролера в нормальному режимі та дозволяє враховувати такі параметри, як інтенсивність звернень до контролера та середній час обслуговування заявки. Однак така СМО недостатньо повно описує роботу контролера, тому що не враховує можливість втрати легітимних пакетів при появі DoS/DDoS-атак.

Для вдосконалення запропонованої моделі доцільно розділити розглянуту СМО на дві системи, які обслуговують заявки на нормальне встановлення з'єднання (коли всі пакети доставлені) і напіввідкриті з'єднання, що видаляються по таймауту. Для поділу вихідного потоку вимог на множину заявок для кожної із систем необхідно ввести критерій, що дозволяє визначити належність заявок до вищеописа-

них типів. Для цього буде використаний той факт, що в більшості випадків час проходження пакета між довільними комутаторами не перевищує деякого порогового значення.

6. Модель, що враховує втрату пакетів у мережі

Розділимо СМО на дві системи: СМО1 та СМО2. Вважатимемо, що перша система описує обслуговування заявок, для яких напіввідкриті з'єднання будуть успішно встановлені після отримання комутатором відповіді контролера, а друга – вимоги, для яких з'єднання не будуть встановлені та після закінчення відведеного таймауту будуть видалені.

Найчастіше час обміну парою пакетів між комутатором і контролером не перевищує поріг T_n. До вимог другого типу відноситимемо заявки, котрим TCP з'єднання перебуває у напіввідкритому стані довше ніж T_n. Позначимо через s і l – кількості сполук першого та другого типів відповідно.

Визначимо співвідношення, що описують стан такої системи. Аналогічно (6) визначимо середню кількість напіввідкритих з'єднань:

$$N = s + l = \alpha_1 + \alpha_2 = \frac{\lambda_1}{\mu_1} + \frac{\lambda_2}{\mu_2}. \tag{7}$$

Як випливає із співвідношення (7), середня кількість напіввідкритих з'єднань є випадковою величиною, що дорівнює сумі двох випадкових величин, що мають пуасонівський закон розподілу. Перша з них описує середню кількість напіввідкритих з'єднань, які не становлять загрози з точки зору атаки. Друга складова являє собою напіввідкриті з'єднання, які не будуть встановлені і через заданий проміжок часу (визначається тайм-аут) будуть видалені, до цього займаючи ресурси контролера. Збільшення кількості таких з'єднань є ознакою атаки.

Далі будемо розглядати в якості заявки не всі пакети, для яких комутатор очікує пакет у відповідь від контролера, а тільки ті, для яких час очікування перевищує порогове значення T_n. Інтенсивність надходження таких заявок визначається співвідношенням:

$$\lambda_2 = \lambda \cdot P_{no}, \tag{8}$$

де λ – інтенсивність пакетів, що надходять, P_{no} - ймовірність появи напіввідкритого з'єднання, яке не буде встановлено.

Параметр P_{no} залежить від якості роботи мережі, яка характеризується ймовірністю втрати пакета мережі P_{nn}. Знайдемо залежність P_{no} від P_{nn}. Нехай подія А полягає в тому, що було втрачено пакет у напрямку від комутатора до контролера, а подія В являє собою втрату пакета від контролера до комутатора. Імовірність події А дорівнює ймовірності втрати пакету в мережі:

$$P(A) = P_{nn}. \tag{9}$$

Так як подія В може наступити тільки тоді, коли не настала подія А, то її ймовірність дорівнює:

$$P(B) = P(\overline{A}) \cdot P_{nn} = (1 - P_{nn}) \cdot P_{nn}. \tag{10}$$

Розглянемо подію С, що полягає у появі напіввідкритого з'єднання другого типу. Вона дорівнює сумі подій А і В. Звідси з урахуванням (9) та (10) отримаємо:

$$\begin{aligned} P_{no} = P(C) = P(A+B) = P(A) + P(B) = \\ = P_{nn} + (1 - P_{nn}) \cdot P_{nn} = P_{nn} + P_{nn} - P_{nn}^2 = 2P_{nn} - P_{nn}^2. \end{aligned} \tag{11}$$

Зі співвідношень (8) і (11) знайдемо інтенсивність потоку вимог другого типу:

$$\lambda_2 = \lambda \cdot P_{no} = \lambda \cdot (2P_{nn} - P_{nn}^2). \tag{12}$$

Комутатор може надсилати декілька копій пакетів доти, доки не буде отримано відповідь контролера. Позначимо кількість таких копій параметром N_{kontr}. Тоді цікава для нас подія полягає в тому, що для жодної з копій не дійде пакет у відповідь, і співвідношення (12) приймає такий вигляд:

$$\lambda_2 = \lambda \cdot P_{no}^{N_{kontr}} = \lambda \cdot (2P_{nn} - P_{nn}^2)^{N_{kontr}}. \tag{13}$$

Оскільки інтенсивність потоку вимог другого типу (наявність атак) пропорційна інтенсивності початкового потоку, він також є пуассонівським.

Середня кількість таких заявок, що знаходяться на обслуговуванні в СМО, визначається другим складником формули (7):

$$l = \frac{\lambda_2}{\mu_2} = \frac{\lambda \cdot P_{nn}^{N_{kontr}}}{\mu_2} = \frac{\lambda(2P_{nn} - P_{nn}^2)^{N_{kontr}}}{\mu_2}, \quad (14)$$

де $\frac{1}{\mu_2}$ – таймаут, відведений на комутаторі встановлення TCP з'єднання, P_{nn} - ймовірність втрати пакета в мережі, N_{kontr} – кількість копій пакетів, що відправляються комутатором.

При використанні даної моделі ознакою атаки є перевищення значення середньої кількості заявок від поточної кількості напіввідкритих з'єднань деякого порогового значення l_{nop}, яке буде відповідати ймовірності вірного виявлення атаки.

Перевагами запропонованої моделі є можливість своєчасного (раннього) виявлення атаки, її здатність адаптуватися до реальних параметрів мережі. При значному збільшенні інтенсивності звернень до контролера кількість втрачених пакетів збільшується пропорційно до ймовірності втрати пакета в мережі. Так як для сучасних мереж ця величина має невелике значення, ефективність виявлення знизиться незначно. Недоліком є те, що несправності мережного обладнання, внаслідок яких збільшується ймовірність втрати пакета в мережі, будуть інтерпретовані як атака. Для того щоб мати можливість ефективно виявляти атаку на практиці, необхідні засоби, що дозволяють визначати значення вихідних параметрів моделі.

Висновки

1. Архітектура мережі 5G не позбавлена потенційних вразливостей з погляду інформаційної безпеки. Контролер як ключовий компонент в управлінні усією інфраструктурою є найуразливішим елементом, атака на який може спричинити критичні для всієї інфраструктури наслідки. Основними загрозами, що виникають з боку мережевих пристроїв, що працюють за принципом програмно-конфігурованої мережі, залишаються варіації таких атак, як "відмова в обслуговуванні", заміна контролера і т.п.

2. Запропоновано реакцію мережі 5G на потоки різних пакетів, у тому числі і на атаки розглядати як функціонування деякої системи масового обслуговування, яка опрацьовує вимоги на обробку пакетів.

3. Розроблено математичну модель мережі 5G у вигляді системи масового обслуговування. Отримано математичну залежність середньої кількості заявок при появі атак.

Література

1. Nick McKeown. Openflow: enabling innovation in campus networks/ Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, Jonathan Turner// ACM SIGCOMM Computer Communication Review, 38[2]. - 2008. – 69–74.

2. OpenFlow Switch Specification Ver 1.5.1, 2016 [accessed January 11, 2016]. https://www.opennetworking.org/images/stories/downloads/sdnresources/ onf-specifications/openflow/openflow-switch-v1.5.1.pdf.

3. Партика Т.Л. Інформаційна безпека/Партика Т.Л., Попов І.І. - Навчальний посібник для студентів закладів середнього професійної освіти. — М.: ФОРУМ: ІНФРА-М. – 2002. − 368с.

4. Лукацкий А. Інформаційна безпека 2015/ Лукацкий А. – Іт-безпека. Стандарти. Засоби захисту. Заходи. № 12. 2013. с.64-69.

5. Ложковский А.Г. Теорія масового обслуговування в телекомунікаціях: підручник / А.Г. Ложковский. – Одеса: ОНАС ім. А. С. Попова: ISBN 978-966-7595-43-3. – 2012. – 112 с.

6. Ложковский А.Г. Моделювання багатоканальної системи обслуговування з організацією черги/ А.Г. Ложковский, Н.С. Салманов, О.В.Вербанов // Східно-європейський журнал передових технологій. – 2007. – №3/6(27). – С.72-76.